

1. Record Nr.	UNINA9910369902103321
Autore	Waghmare Charles
Titolo	Augmenting Customer Experience with SharePoint Online : Building Portals and Practices to Improve Usability / / by Charles Waghmare
Pubbl/distr/stampa	Berkeley, CA : , : Apress : , : Imprint : Apress, , 2020
ISBN	9781484255346 1484255348
Edizione	[1st ed. 2020.]
Descrizione fisica	1 online resource (152 pages)
Disciplina	006.78
Soggetti	Microsoft software Microsoft .NET Framework Microsoft and .NET
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Includes index.
Nota di bibliografia	Includes bibliographical references.
Nota di contenuto	Chapter 1: Introducing SharePoint Online Features -- Chapter 2: Office 365 and SharePoint Online for Digital Customer Experience -- Chapter 3: Exploring Digital Customer Experience -- Chapter 4: Using UX and UIs to Develop Smart Portals -- Chapter 5: Building Knowledge systems using SharePoint Online -- Chapter 6: AI in DCX. .
Sommario/riassunto	Build, enrich, and transform customer experience using SharePoint Online. This book will discuss different SharePoint Online approaches that you can use to enhance customer experience, including digital portals, enterprise content management, Microsoft Teams and much more. Augmenting Customer Experience with SharePoint Online starts with an introduction to SharePoint Online features you can adopt to create better digital customer experience and transformation. Next, you will learn about augmentation for user and customer experience followed by guidelines and methods to develop smart and intelligent portals. Moving forward, you will cover enterprise and web content management in detail along with the challenges and benefits of using SharePoint Online. The partner ecosystem is discussed next with a detailed discussion on working with suppliers, partners, and vendors. Along the way, you will see how to create smart solutions using SharePoint Online and how to manage customer references. Finally, you

will go through the use of SharePoint Online in different business sectors with the help of case studies. After reading the book, you will be able to adopt SharePoint Online features to augment customer and user experience. You will: Augment customer experience Create smart and intelligent portals for various business needs Efficiently manage enterprise and web content Enhance your partner ecosystem for better collaboration Build SharePoint Online solutions.

2. Record Nr.	UNINA9911020189803321
Autore	Held Gilbert <1943->
Titolo	Securing wireless LANs : a practical guide for network managers, LAN administrators, and the home office user / / Gilbert Held
Pubbl/distr/stampa	Hoboken, NJ, : J. Wiley, c2003
ISBN	9786610272488 9781280272486 1280272481 9780470299784 0470299789 9780470869680 0470869682 9780470869697 0470869690
Descrizione fisica	1 online resource (274 p.)
Disciplina	005.8
Soggetti	Wireless LANs - Security measures
Lingua di pubblicazione	Inglese
Formato	Materiale a stampa
Livello bibliografico	Monografia
Note generali	Description based upon print version of record.
Nota di bibliografia	Includes bibliographical references and index.
Nota di contenuto	securing wireless LANs; contents; Preface; Acknowledgements; Chapter 1 Introduction to Wireless LANs; 1.1 SECURING THE INSECURE; 1.1.1 AAE AND A FUNCTIONS; 1.1.2 AUTHENTICATION; 1.1.3 AUTHORIZATION; 1.1.4 ENCRYPTION; 1.1.5 ACCOUNTING; 1.1.6 PRACTICAL NETWORK PROTECTION METHODS; 1.2 NETWORK ARCHITECTURE; 1.2.1 BASIC NETWORKING DEVICES; 1.2.2 THE

WIRELESS LAN STATION; 1.2.3 THE ACCESS POINT; 1.2.4 THE WIRELESS BRIDGE; 1.2.5 THE WIRELESS ROUTER; 1.2.6 THE BASIC SERVICE SET; 1.2.7 THE EXTENDED SERVICE SET (ESS); 1.2.8 STATION SERVICES; 1.3 IEEE WIRELESS LAN STANDARDS
1.3.1 THE BASIC IEEE 802.11 STANDARD1.3.2 802.11B; 1.3.3 802.11A; 1.3.4 802.11C; 1.3.5 802.11D; 1.3.6 802.11E; 1.3.7 802.11F; 1.3.8 802.11G; 1.3.9 802.11H; 1.3.10 802.11I; 1.4 BOOK PREVIEW; 1.4.1 FRAME FORMATS AND BASIC SECURITY OPERATIONS; 1.4.2 UNDERSTANDING WIRELESS SIGNALS; 1.4.3 UNDERSTANDING WEP; 1.4.4 SECURITY RISKS; 1.4.5 PROPRIETARY SECURITY ENHANCEMENT TECHNIQUES; 1.4.6 STANDARDS BASED SECURITY; Chapter 2 Frame Formats and Basic Security Operation; 2.1 FRAME FORMATS; 2.1.1 BASIC FRAME FORMAT; 2.1.2 FRAME CONTROL FIELD; 2.1.3 CONTROL FRAMES; 2.1.4 MANAGEMENT FRAMES
2.1.5 THE AUTHENTICATION PROCESS2.2 WEP AND PRIVACY; 2.2.1 MISCONCEPTIONS; 2.2.2 DEVELOPMENT CONSTRAINTS; 2.2.3 DEFICIENCIES; Chapter 3 Understanding Wireless Signals; 3.1 THE WIRELESS RF SPECTRUM AND BASIC MEASUREMENTS; 3.1.1 FREQUENCY; 3.1.2 PERIOD AND WAVELENGTH; 3.1.3 BANDWIDTH; 3.1.4 THE FREQUENCY SPECTRUM; 3.1.5 POWER MEASUREMENTS; 3.1.6 POWER LEVEL; 3.1.7 SIGNAL-TO-NOISE RATIO; 3.2 ANTENNA BASICS; 3.2.1 BASIC OPERATION; 3.2.2 CATEGORIES; 3.2.3 ANTENNA GAIN; 3.2.4 DIRECTIONALITY AND EIRP; 3.2.5 POWER LEVELS; 3.2.6 PROPAGATION LOSS; 3.2.7 INCREASING ANTENNA GAIN; 3.2.8 POWER LIMITS 3.2.9 RECEIVER SENSITIVITY3.2.10 REDUCING EMITTED RADIATION; 3.2.11 HORIZONTAL TRANSMISSION DISTANCE; 3.2.12 EQUIPMENT POSITIONING; 3.2.13 USING MONITORING EQUIPMENT; Chapter 4 Understanding WEP; 4.1 THE WEP FRAME BODY; 4.1.1 THE IV; 4.1.2 THE ICV; 4.1.3 THE NAKED DEFAULT; 4.1.4 WEP KEY LIMITATIONS; 4.2 LOCATING AND OBSERVING WIRELESS LAN TRAFFIC; 4.2.1 NETWORK STUMBLER; 4.2.2 MONITORING WITH AIROPEEK; 4.3 RC4; 4.3.1 OVERVIEW; 4.3.2 OPERATION; 4.3.3 ILLUSTRATIVE EXAMPLE; 4.3.4 STRENGTHS AND WEAKNESSES; 4.4 WEP WEAKNESS; 4.4.1 UNSAFE AT ANY SIZE; 4.4.2 THE INSECURITY OF 802.11
4.4.3 EXPLOITING RC4 WEAKNESS4.4.4 BREAKING WEP; 4.4.5 AIRSNORT; 4.4.6 WEPCRACK; Chapter 5 Security Risks and Countermeasures; 5.1 THE SSID; 5.1.1 OVERVIEW; 5.1.2 OVERRIDING THE SSID; 5.1.3 OBTAINING THE SSID; 5.1.4 COUNTERMEASURES; 5.2 EAVESDROPPING; 5.2.1 OVERVIEW; 5.2.2 THREATS; 5.2.3 COUNTERMEASURES; 5.3 MASQUERADE; 5.3.1 OVERVIEW; 5.3.2 COUNTERMEASURES; 5.4 DATA MODIFICATION; 5.4.1 OVERVIEW; 5.4.2 COUNTERMEASURES; 5.5 FILE SHARING; 5.5.1 OVERVIEW; 5.5.2 WINDOWS 95; 5.5.3 WINDOWS 2000; 5.5.4 COUNTERMEASURES; 5.6 JAMMING; 5.6.1 OVERVIEW; 5.6.2 COUNTERMEASURES; 5.7 ENCRYPTION ATTACKS
5.7.1 OVERVIEW

Sommario/riassunto

Wireless LANs will enable small teams and communities to communicate via their mobile devices without cables. This new technology will facilitate communication in small businesses/teams such as in hospitals, on construction sites, warehouses, etc. Held provides a comprehensive guide to the implementation, planning and monitoring of all aspects of wireless LAN security in small offices/small to medium business (SMBs). Securing Wireless LANs is timely in addressing the security issues of this important new technology and equips its readers with the tools they need to make the appro
